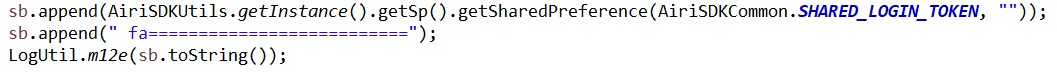
1. Searching for logging functions, I found that most of them are wrapped in some logger for both the app and it’s SDK, for example:



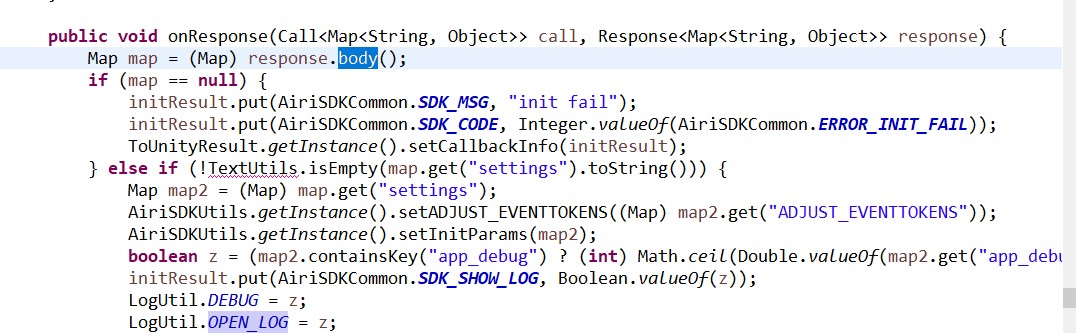
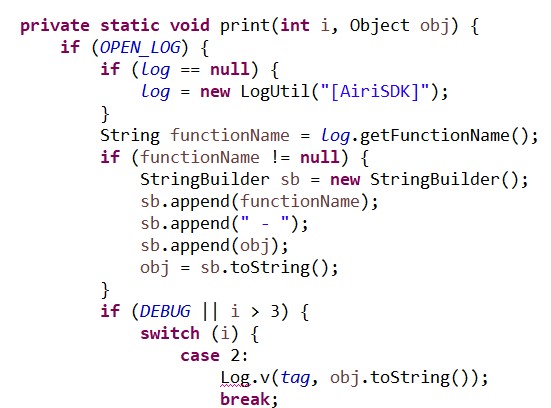
So I tried to search some usage of this Loggers.



Mostly I did not found anything. But there is AiriSDK in this app, that’s responsible for logging into app, that does save some data in logs.

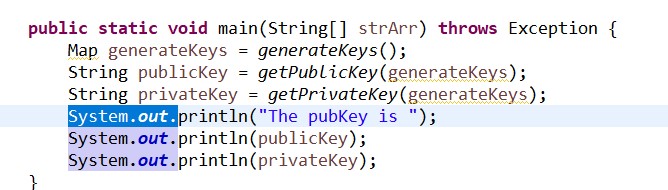


But there is a big BUT in this one. All functions of logging for this sdk refer to print function, that has a flag OPEN\_LOG in it, that is responsible for actually logging information.



From what I saw, the actual settings for logging are stored on server and logs are enabled/disabled based on what the app receives in responses from server.

1. Here is something very weird:



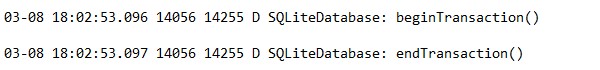
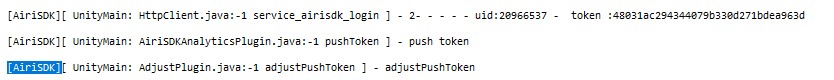
Seems like a huuuuge vulnerability. But as I understood, that’s only for debugging. Most usage of RSAUtils was like this:



So main is never actually touched. Still, it could be removed just cause it’s not very safe.

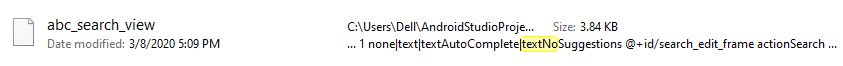
1. Couldn’t find any journals in data/data/com.YostaR.Arknights folder and subfolder. But I looked through real-time logs with adb logcat command.

Here is what I found:



Not the worst, but still some info gets leaked.

1. Only SDK that I found info on vulnerabilities of was facebook SDK (wow, what a surprise). All SDKs were up to date.
2. There are no fields in this app that require confidential data to be put in. All logging in procedure goes through AiriSDK, which in itself uses social networks accounts to log in. But I found textNoSuggestions flag, but it was for search field.



1. Here are providers from AndroidManifest.xml.







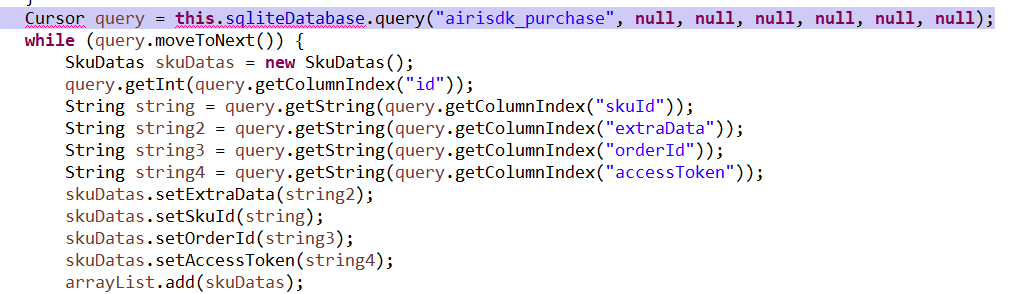


All providers have android:exported=false.



I found only one permission with protectionLevel. For cloud to device messages.

1. Did not find any usages of ContentProviders, but found some for Cursor:



1. Did not find any fields with “textPassword” type / fields that require hiding confidential info.
2. Backup seems to be allowed:



And all confidential info is fully intact in backup:

